Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

In the Matter of	)	
	)	
Protecting the Privacy of Customers	)	WC Docket No. 16-106
of Broadband and Other	)	
Telecommunications Services	)	

REPLY COMMENTS OF THE INTERNET ASSOCIATION

The Internet Association ("IA") respectfully submits these reply comments in response to the petitions[1] that ask the Federal Communications Commission ("FCC" or "Commission") to reconsider the rules governing broadband Internet service providers ("ISPs") adopted in the *2016 ISP Privacy Report & Order*,[2] as well as the oppositions to those petitions.

IA represents the interests of America's leading Internet companies and their global community of users. IA supports policy solutions that strengthen and protect Internet freedom, foster innovation and economic growth, and empower users. IA is also committed to protecting users' online privacy by providing cutting-edge tools that empower users to make choices about how they view content online.

IA encourages the Commission to keep three fundamental principles in mind as it reconsiders its ISP privacy and security rules. *First*, the Commission should not disturb its conclusion that Section 222 of the Communications Act does not apply to providers of edge

[1] *See, e.g.*, Petition for Reconsideration of USTA, WC Docket No. 16-106 (filed Jan. 3, 2017) ("USTA Petition"); Petition for Reconsideration of NCTA, WC Docket No. 16-106 (filed Jan. 3, 2017) ("NCTA Petition"); Petition for Reconsideration of Competitive Carriers Association, WC Docket No. 16-106 (filed Jan. 3, 2017); Petition for Reconsideration of CTIA, WC Docket No. 16-106 (filed Jan. 3, 2017); Petition for Reconsideration of Oracle, WC Docket No. 16-106 (filed Jan. 3, 2017) ("Oracle Petition").

[2] *Protecting the Privacy of Customers of Broadband and Other Telecommunications Services*, WC Docket No. 16-106, Report and Order, 31 FCC Rcd 13911 (rel. Nov. 2, 2016) ("*2016 ISP Privacy Report & Order*").

services and other non-Title II offerings. *Second*, the Commission should seek to more closely align its ISP privacy and security rules with the Federal Trade Commission's ("FTC") time-tested data privacy and security framework, including for browsing history and app usage data. Doing so would help minimize confusion and uncertainty within the Internet ecosystem, and it would better protect consumers and encourage innovation than a host of prescriptive rules. *Finally*, any continued departure from the FTC's framework should be grounded exclusively in the regulatory, policy, and economic factors that actually distinguish ISP and edge markets.

I. THE FCC SHOULD NOT DISTURB ITS CONCLUSION THAT SECTION 222 DOES NOT APPLY TO PROVIDERS OF EDGE SERVICES AND OTHER NON-TITLE II OFFERINGS.

The *2016 ISP Privacy Report & Order* concluded that the Commission's privacy and security rules do not apply to edge providers.[3] That conclusion, uncontested by the petitions for reconsideration,[4] is correct. The Commission should leave it undisturbed.

The FCC lacks statutory authority to regulate the privacy and security practices of edge providers. Section 222 of the Communications Act applies to "telecommunications carriers."[5] A "telecommunications carrier" is an entity that provides "telecommunication services," which is "the offering of telecommunications for a fee directly to the public, or to such classes of users as to be effectively available directly to the public, regardless of the facilities used."[6] In the *2015*

[3] *See id.* ¶ 40.
[4] In contrast, organizations across the political and economic spectrum agree that it would be unlawful to apply Section 222 to edge services. *See, e.g.*, Reply Comments of the Internet Association, WC Docket No. 16-106, at 2-3 (filed Jul. 6, 2016) (internal citations omitted) ("IA Reply Comments") (collecting comments from a diverse assortment of civil society organizations, academics, trade associations, and technology companies).
[5] 47 U.S.C. § 222(a) ("Every *telecommunications carrier* has a duty to protect the confidentiality of proprietary information of, and relating to, other telecommunication carriers, equipment manufacturers, and customers, including telecommunication carriers reselling telecommunications services provided by a telecommunications carrier.") (emphasis added).
[6] 47 U.S.C. § 153(53).

Open Internet Order, the Commission reclassified retail broadband Internet access service as a telecommunications service, but it has taken no similar action for Internet edge services."[7]

Applying Section 222 to edge services is not only unlawful, but also unnecessary. The FCC's reclassification of ISPs as Title II common carriers stripped the FTC of jurisdiction to regulate ISPs' privacy practices.[8] This arguably created a need for the FCC to take action in this proceeding with respect to ISPs. But no similar justification applies for edge services. The FTC currently exercises robust oversight of non-Title II services on privacy, security, and other consumer protection issues, as do state regulators.[9] There is thus no risk of any enforcement "gap" for edge providers. Adopting additional data privacy and security requirements on edge services and other non-Title II offerings would upend the current regulatory framework for those services without providing meaningful additional benefits for consumers.

Although the FCC's ISP privacy and security rules clearly exclude edge services, Chairman Pai and Commissioner O'Rielly have raised concerns regarding the potential effect of the rules on edge providers, the Internet of Things ("IoT"), and the FTC's framework.[10] On reconsideration, the Commission may consider reiterating that its ISP privacy and security rules are not intended to disturb the existing legal framework governing edge providers—whether or not in connection with IoT offerings. Although the Communications Act, the *2016 ISP Privacy*

---

[7] *See, e.g.*, *Protecting and Promoting the Open Internet*, GN Docket No. 14-28, Report and Order on Remand, Declaratory Ruling, and Order, 30 FCC Rcd. 5601 ¶ 377 (2015) ("*2015 Open Internet Order*") ("We find that these services identified in the record—email, cloud-based storage, and spam protection—are separable information services. We conclude that e-mail accounts and cloud-based storage provided along with broadband Internet access services are akin to voicemail services offered along with traditional telephone service.").

[8] 15 U.S.C. § 45(a)(2) (creating an exception to FTC's Section 5 jurisdiction with respect to "common carriers subject to the Acts to regulate commerce"); *Fed. Trade Comm'n v. AT&T Mobility LLC*, 835 F.3d 993 (9th Cir. 2016).

[9] *See, e.g.*, Ark. Code Ann. § 4-110-104(b); Cal. Civ. Code § 1798.81.5; MD Code Ann. § 14-3503(a).

[10] *See 2016 ISP Privacy Report & Order*, Dissenting Statement of Commissioner (now Chairman) Pai, Dissenting Statement of Commissioner O'Rielly.

Report & Order, and the *2015 Open Internet Order* plainly forbid such an outcome, IA welcomes further clarification to obviate any unnecessary confusion with respect to edge services.

II. THE FCC SHOULD SEEK TO FURTHER HARMONIZE ITS RULES WITH THE FTC'S PRIVACY AND SECURITY FRAMEWORK.

The FTC's flexible, time-tested privacy framework has been a major success story.[11] As discussed extensively in the record and recognized by a majority of the current FCC Commissioners, the FTC's case-by-case approach has served consumers well.[12] The FTC has also zealously enforced its framework against parties that fail to meet the Section 5 requirements.[13] Even if the Commission determines that the ISP privacy and security rules may ultimately need to differ in some respects from the requirements applicable to edge providers, further harmonizing the frameworks would minimize any unnecessary confusion, protect consumers, and encourage innovation than would a host of prescriptive rules applicable to ISPs.

Browsing History and App Usage Data. Numerous parties recognize that the FCC's ISP privacy and security requirements conflict with the FTC's framework with respect to "sensitive" data.[14] For example, as Chairman Pai and Commissioner O'Rielly noted, the ISP privacy and data security rules represent a "significant departure from the FTC approach, which is the basis for current expectations,"[15] by classifying browsing history and app usage data as "sensitive."

---

[11] *See* Comments of the Internet Association, WC Docket No. 16-106, at 4-6 (filed May 27, 2016) ("IA Comments").
[12] *See 2016 ISP Privacy Report & Order*, Dissenting Statement of Commissioner (now Chairman) Pai, Dissenting Statement of Commissioner O'Rielly.
[13] *See* IA Comments at 7-8.
[14] *See, e.g.*, Comments of the Internet Commerce Coalition, WC Docket No. 16-106, at 1-2 (filed Mar. 6, 2017); USTA Petition at 4-12; NCTA Petition at 12-21.
[15] *2016 ISP Privacy Report & Order*, Dissenting Statement of Commissioner O'Rielly; *see also id.* Dissenting Statement of Commissioner (now Chairman) Pai.

Under the FTC's approach, "reasonableness" is the lodestar, and context and content are the key considerations. The relevant issue is the sensitivity of the specific data, not the entity obtaining or using the data or the channel through which it is obtained. Applying this framework, the FTC has recognized the sensitivity of "data about children, financial and health information, Social Security numbers, and certain geolocation data."[16] It has not, however, categorically deemed browsing history and app usage information to be "sensitive."

The FTC's conclusion makes sense. Browsing history and app usage information are qualitatively different from the other data elements that the FCC and FTC have categorized as "sensitive"—social security numbers, financial data, health data, children's data, etc. The latter is more likely to have a direct connection to concrete consumer injury. Identity theft may result from the unauthorized disclosure of social security numbers, and financial harm can flow from the release of payment card information.

For this reason, information traditionally considered "sensitive" is subject to robust operational and regulatory protections. It typically enters the stream of commerce through limited, trusted channels—banks and medical providers, for example—and is customarily encrypted in online transactions. And express, detailed federal statutory protections sometimes accompany traditionally "sensitive" data categories, which are defined narrowly. Examples include the Health Insurance Portability and Accountability Act (health),[17] Gramm-Leach-Bliley Act (financial),[18] Privacy Act (social security),[19] Children's Online Privacy Protection Act (children),[20] and Fair Credit Reporting Act (credit history).[21]

---

[16] *See* Federal Trade Commission, *Protecting Consumer Privacy in an Era of Rapid Change: Recommendations for Business and Policymakers* 47 (2012).
[17] 42 U.S.C. § 1320d–6.
[18] 15 U.S.C. §§ 6801–6809.
[19] 5 U.S.C. § 552a.
[20] 15 U.S.C. §§ 6501–6505.

These factors are entirely absent in the context of browsing history and app usage data—overbroad categories that cover even daily sports scores and routine weather updates. In online transactions, data is often accessed at multiple points, including through browsers, applications, operating systems, edge providers, and ISPs.[22] The potential harm associated with unauthorized access of browsing and app information is highly speculative and dependent on the particulars of the situation. And Congress has refrained from enacting categorical statutory protections with respect to this data.

III. ANY DEPARTURES FROM THE FTC'S FRAMEWORK SHOULD BE STRICTLY CIRCUMSCRIBED TO THE UNIQUE ROLE THAT ISPS HAVE IN THE INTERNET ECOSYSTEM.

While IA supports further harmonization with the FTC's framework, it disagrees with comments on the record that incorrectly suggest equivalence between ISPs and edge providers.[23] There are many good reasons for the Commission to better align the ISP privacy and security rules with the FTC's framework, but a wrongheaded comparison to edge services is not one of them. Edge providers are a heterogeneous class of entities that provide a wide range of different services to varying consumer segments; they are materially different from ISPs, a concretely defined category of providers that share important, common service features. Accordingly, the Commission's reconsideration of the ISP privacy and security rules should not be driven by misplaced analogies to edge providers' practices, but rather should acknowledge the important economic, technical, and regulatory factors that differentiate ISPs and edge services.

For example, this proceeding grew directly out of the *2015 Open Internet Order*, where the FCC stated that the ISPs' unique role as "gatekeepers" of traffic flowing between consumers

---

[21] 15 U.S.C. §§ 1681–1681x.
[22] *See, e.g.*, Comments of zeotap GmbH, WC Docket No. 16-106, at 9 (filed Mar. 3, 2017).
[23] *See, e.g.*, Oracle Petition at 3.

and edge providers could pose concerns.[24] The Commission reasoned that due to this privileged position, ISPs may discriminate in favor of their own content, extract tolls from edge providers, or target competing services.[25] This was also the basis for the Commission's anti- blocking, throttling, and prioritization rules (and a core justification upon which the D.C. Circuit upheld the *2015 Open Internet Order*).[26]

Large fixed costs also affect the competitiveness of the ISP industry and contribute to ISPs' gatekeeping role. Significant capital expenditures involve installing poles and other facilities, digging trenches, laying conduit, locating and constructing wireless antennas, and conducting other infrastructure deployment. These activities require a large upfront spend and economies of scale. ISPs must also incur significant operational expenses, such as hiring and training staff to provide marketing, billing, technical, and customer support.

Regulatory barriers to entry in the ISP market also exist.[27] New entrants may need to obtain approval from local governments for access to publicly owned rights-of-way to allow them to place wires above or below property, and to locate their wireless facilities. Similarly, new entrants might need to contract with public utilities to rent space on utility poles or in underground spaces. Moreover, the scarcity of spectrum limits the provision of wireless voice and internet services.

The ISP market can also be characterized by high consumer switching costs.[28] To switch ISPs, a customer would need to first cancel the service agreement with her existing provider and then set up her new service (assuming a sufficient substitute is available). Not only is this typically a multi-step process that frequently involves phone calls and installation appointments,

[24] *See 2015 Open Internet Order* ¶ 20.
[25] *Id.* ¶ 86.
[26] *Id.* ¶ 102; *see U.S. Telecom Ass'n v. FCC*, 825 F.3d 674, 694 (D.C. Cir. 2016).
[27] *See* IA Reply Comments at 9.
[28] *See 2016 ISP Privacy Report & Order* ¶ 36.

but there are also financial considerations. Customers may need to put down a new deposit and pay a set-up or installation fee to the new ISP, and they also may have to pay an early termination fee to the old provider. When broadband customers have been asked about the factors that might keep them from switching service, respondents with the choice of multiple providers have stated factors such as set up or installation fees, the process of getting new service installed, making a new deposit, and having to change their current bundle of Internet, TV, and phone service.[29]

By contrast, barriers to entry and switching costs do not restrict the competitive market for edge services. An app developer and other edge providers need little more than a standard Internet-connected computer. Consumers can easily decide to use (or not use) any website or app, or can chose to use multiple edge providers—and the robust state of competition online shows that they are doing just that.[30] Switching edge service providers normally involves a few mouse clicks. Moreover, most of an edge service users' activity involves visiting websites or using applications that do not charge any fees. Users are not tied to these websites or applications and can choose to pick a new online publication, search engine, mobile application, or email provider with ease (including any edge services offered by ISPs).

The differences between ISPs and edge providers offer some guidance on how the FCC should resolve the petitions for reconsideration. As the Commission seeks to further harmonize its rules with the FTC's framework, it should rely on the FTC's context-specific approach to sensitive data, not any purported equivalence between ISPs and edge providers. Furthermore, to the extent that the Commission departs from the FTC's framework, it should ground such

[29] *See* IA Reply Comments at 9-10.
[30] *See 2016 ISP Privacy Report & Order* ¶ 36 ("In addition, consumers have a choice in deciding each time whether to use—and thus reveal information—to an edge provider ... whereas that is not an option with respect to their BIAS provider when using the service.").

departures on the ISP-specific factors already identified by the Commission—*e.g.*, ISPs' gatekeeping role, barriers to entry in the broadband market, and switching costs associated with consumer data plans.

This approach recognizes the multiple services and roles that an ISP may have. Where ISPs offer edge services, they would be governed by the same set of rules as edge providers. When offering ISP services, to the extent that an ISP may seek to leverage any gatekeeping position to favor their offerings at the expense of competing services, the FCC may be justified in addressing imposing tailored requirements.

* * *

For the foregoing reasons, the Commission should seek to further harmonize the ISP privacy and security rules with the FTC's framework in a manner that avoids disruption to edge services.

Respectfully submitted,

/s/ *Mark W. Brennan*

Mark W. Brennan
Arpan A. Sura
Hogan Lovells US LLP
555 Thirteenth St. NW
Washington, DC 20004
(202) 637-6409

Counsel for the Internet Association

Abigail Slater
General Counsel
The Internet Association
1333 H Street NW
West Tower, Floor 12
Washington, DC 20005
(202) 770-0023

March 14, 2017